

**DRAFT**

**Industrial Control System Security Capabilities Profile  
22 May 2003**

**Process Control  
Security Requirements Forum  
(PCSRF)**

**Security Capabilities Profile  
for  
Industrial Control Systems**

**22 May, 2003**

**DRAFT**

## DRAFT

# Industrial Control System Security Capabilities Profile 22 May 2003

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>3</b>
1.1.	INITIATIVE PURPOSE .....	3
1.2.	DOCUMENT PURPOSE .....	4
1.3.	SCOPE OF APPLICATION .....	5
1.4.	INDUSTRIAL CONTROL SYSTEM DEFINITION .....	5
1.5.	UNDERSTANDING AND APPLYING THIS DOCUMENT .....	6
1.5.1.	<i>How this Document was Developed</i> .....	6
1.5.2.	<i>Intended Usage</i> .....	6
1.5.3.	<i>Difference between Capability and Configuration</i> .....	8
1.6.	RELATIONSHIP OF THIS DOCUMENT TO OTHER ICS SECURITY INITIATIVES .....	9
1.6.1.	<i>Relationship with the PCSRF</i> .....	9
1.6.2.	<i>Relationship with SP99</i> .....	10
1.6.3.	<i>Relationship to NIAP &amp; Common Criteria Recognition Arrangement (CCRA)</i> .....	10
1.6.4.	<i>Relationship to industry-specific initiatives (e.g., CIDX, API, GTI, EPRI, NMCS)</i> .....	10
1.7.	READING THIS DOCUMENT .....	11
<b>2.</b>	<b>ICS SYSTEM DEFINITION AND DESCRIPTION .....</b>	<b>12</b>
<b>3.</b>	<b>OPERATIONAL SECURITY ENVIRONMENT .....</b>	<b>15</b>
3.1.	SECURE USAGE AND ENVIRONMENT ASSUMPTIONS .....	15
3.2.	VULNERABILITIES .....	17
3.3.	REGULATORY MANDATES & POLICY .....	19
<b>4.</b>	<b>INDUSTRIAL CONTROL SYSTEM CAPABILITY OBJECTIVES.....</b>	<b>20</b>
4.1.	ICS NON-TECHNICAL OPERATIONS OBJECTIVES .....	20
4.2.	ICS TECHNOLOGY-BASED OBJECTIVES .....	22
<b>5.</b>	<b>CONTROL SYSTEM COMPONENT SECURITY CAPABILITY REQUIREMENTS .....</b>	<b>25</b>
5.1.	SECURITY FUNCTIONAL IMPLEMENTATION REQUIREMENTS .....	25
5.1.1.	<i>ICS Security-Related Event Recording and Auditing</i> .....	25
5.1.2.	<i>Communication Channels and Interconnects</i> .....	26
5.1.3.	<i>Boundary Defense Devices</i> .....	26
5.1.4.	<i>Network Addressable Field Devices</i> .....	27
5.1.5.	<i>Control System Operator Command Console</i> .....	28
5.2.	SECURITY VERIFICATION, OPERATION AND MAINTENANCE ASSURANCE REQUIREMENTS .....	30
5.2.1.	<i>ICS Policy Documentation</i> .....	30
5.2.2.	<i>Architecture Documentation</i> .....	30
5.2.3.	<i>Configuration Documentation</i> .....	31
5.2.4.	<i>Design Documentation</i> .....	31
5.2.5.	<i>System Testing</i> .....	31
5.2.6.	<i>Residual Risk Assessment</i> .....	32
<b>6.</b>	<b>APPENDIX I – PROCESS CONTROL SYSTEMS AND INDUSTRIES OVERVIEW.....</b>	<b>33</b>
6.1.	DCS COMPONENT CHARACTERIZATION .....	34
6.2.	SCADA COMPONENT CHARACTERIZATION.....	34
<b>7.</b>	<b>APPENDIX II – GLOSSARY OF TERMS – GENERIC COMPOSITE INDUSTRIAL CONTROL SYSTEM NETWORK ARCHITECTURE.....</b>	<b>36</b>

DRAFT

# 1. Introduction

## 1.1. Initiative Purpose

The National Information Assurance Partnership (NIAP – partnership between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST)), as part of the Critical Infrastructure Protection Program, provides technical support and guidance to industry to improve the information technology security posture of the systems and supporting operations that comprise the US national critical information infrastructure. One component of this effort addresses computer and communications security<sup>1</sup> for the networked digital process control systems used to provide or support industrial operations. The NIST Intelligent Systems Division of the Manufacturing Engineering Laboratory, the NIST Information Technology Laboratory and the NIST Electrical and Electronics Engineering Laboratory comprise this component, and are working with industry to incorporate comprehensive end-to-end security engineering into the life-cycle processes of process control systems and the components that comprise such systems.<sup>2</sup>

The goal of this effort is to characterize the minimal security capabilities to be provided by the product components that comprise an Industrial Control System (ICS), and the minimal security capabilities that must be exhibited by the ICS after the product components have been integrated together to form an ICS. This effort is being carried out through the Process Control Security Requirements Forum (PCSRF). The outcome of this effort will be a set of security capabilities that can be applied by the control system industrial sectors to aid in the acquisition, integration and operation of ICSs.

The PCSRF is a working group operating under the NIAP. The PCSRF is comprised of representative organizations from the various sectors that make up the US process control industry (i.e., vendors that design, develop, and integrate components and systems for the industry), as well as representatives from companies that use these system. The PCSRF is working with security professionals to assess vulnerabilities and establish appropriate strategies for the development of policies and countermeasures to be employed through combinations of technology and procedural mechanisms.

---

<sup>1</sup> Computer and Communication Security is inclusive of all devices implemented through combinations of hardware, software and firmware, and, which provide or support security-relevant functions of the industrial control system. These functions may also have indirect impact on safety-critical functions of the industrial control system.

<sup>2</sup> End-to-end security engineering in life-cycle processes refers to defining criteria that establishes a basis for the following activities: definition of acquisition requirements; definition of development and integration requirements; definition of verification processes such as certification and accreditation to ensure that solutions are appropriately matched with the operating environment; and the definition of ongoing assessment and adjustment activities to ensure that the desired level of security is maintained as systems evolve through upgrades and replacements due to either technology changes or changes resulting from new threats in the operating environment.

## 1.2. Document Purpose

The document addresses those issues associated with presenting and justifying a *security assurance case* as it applies to day-to-day ICS operations. The security assurance case serves exactly the same purpose as a safety assurance case<sup>3</sup>: it presents *assertions* in regards to the critical capabilities that the system must possess; it provides a body of supporting *evidence* which illustrates that the critical capabilities have been achieved; it provides a set of arguments, or *rationale*, which links the claims to the evidence. The collection of assertions, evidence and rationale enables demonstration of due diligence in justifying that an acceptable level of risk has been achieved.

The security assurance case focuses on presenting assertions, evidence and rationale as follows:

- Statement of the Security Problem: Assertions about the ICS are stated in the form of assumptions about the operational environment and intended use of the ICS, in the form of vulnerabilities in the ICS and the technologies and process used to build operate and maintain the ICS, and in the form of policies, directives and mandates to which the ICS must comply.
- Statement of the Solution to the Security Problem: Assertions about the *protection mechanisms*<sup>4</sup> and *assurance measures*<sup>5</sup> deemed as necessary and sufficient to address the stated security problem are identified and described. The protection mechanisms can be stated in varying degrees of specificity; starting with a high-level statement of objectives, followed by intermediate-level statements of functional and assurance requirements, and finally low-level statements describing the implemented functions and assurance measures.
- Substantiation of the Solution: Rationale demonstrates complete traceability between the statements of the security problem down to the statements of the security solution. The rationale also presents the argument that the implemented mechanisms as a whole are necessary and sufficient to solve the stated security problem.

A security assurance case generates a significant amount of information that must be organized for presentation to the various stakeholders involved with the development, verification and operation of the system once it becomes operational. The Common

---

<sup>3</sup> Safety assurance cases are commonly used by the industrial control sectors and aerospace industries to demonstrate conformance to/compliance with mandated policies specific to operations in those sectors and industries.

<sup>4</sup> A protection mechanism may be implemented through a combination of technology based (i.e. computer-based) mechanisms and procedural functions. With regard to computer based mechanisms, they may in turn be implemented in any combination of hardware, software or firmware.

<sup>5</sup> Assurance measures are the activities conducted to reach a conclusion that the required capabilities have been implemented in accordance with their requirements. Assurance measures include the generation of evidence required to support the activities.

Criteria for Information Technology Security Evaluation (CC/ISO 15408) defines a security specification framework (called a Protection Profile) which provides a standardized template for organizing and specifying security criteria, and catalogs of functional and assurance criteria that is used to populate the template. This document incorporates the concepts of an ISO 15408-compliant Protection Profile (PP) but differs from the PP in several ways:

1. This document contains information that exceeds the scope of information required in a CC-compliant Protection Profile;
2. This document has a structure that differs from a CC-compliant Protection Profile;
3. This document avoids the use of CC-specific terms and phrases.

NIST intends that this document will serve as a means to reach consensus within and across industries regarding the minimal set of security capabilities present in a secure ICS. After that goal is met, this document and its derivatives will serve as a basis for developing ISO 15408-compliant Protection Profiles to aid in development and verification of the security capabilities of ICS systems and product components.

### **1.3. Scope of Application**

This document discusses security issues and capabilities relevant to those industries regarded as components of the national critical information infrastructure. Candidate industries include the electric utilities, discrete parts manufacturing, petroleum (oil & gas), water, waste, chemicals, pharmaceuticals, pulp & paper, and metals and mining.

### **1.4. Industrial Control System Definition**

An ICS can be characterized as a distributed collection of components that provide the following basic functions to control a complex process:

- Measurement – data collection
- Control – data assessment, information generation and response determination
- Manipulation – automatic or manual response execution
- Human-machine interface – processing of inputs from and presentation of information to human operators.

*Application Note: Proposed “view-ability and manipulation of controls”.*

The functions described above are referred to as continuous steady-state functions. While this document focuses on maintaining a continuous secure steady-state, it is also necessary to address the ability to install, configure and transition the ICS from a secure dormant state to its secure continuous steady-state and finally, the security capabilities required to support the ICS transition from the secure continuous steady-state to a secure shutdown state. These functions can be categorized as:

- Startup, initial condition or set-point establishment

- System and process behavior management controls, discrete event logging, configuration and component maintenance and changes
- Failure modes, secure fail-over, and secure recovery
- Shutdown
- Archive and backup

*Application Note: The presentation of material in lines 101-113 requires discussion.*

## **1.5. Understanding and Applying this Document**

This section discusses the methods used to collect the information in this document and discusses application of this document to develop, integrate and operate secure ICSs.

### **1.5.1. How this Document was Developed**

This document was developed through a series of technical information exchanges facilitated by NIST. The information exchanges were conducted through a variety of face-to-face meetings, teleconferences, workshops and industrial control system facility tours. Meetings have been convened at NIST headquarters, at industry conferences and at sector-specific workshops.

The purpose of these industry-focused information exchanges was to capture as much information as possible related to the present state of ICS operations. This type of information exchanges included:

- Discussion of fundamental principles of DCS and SCADA;
- Discussion of the unique aspects and characteristics of the technology employed in ICS as compared to the application of technology for more traditional computer and communications systems;
- Discussion of ICS vulnerabilities;
- Discussion of desired functionality and technology capability.

### **1.5.2. Intended Usage**

This document will support the following technical activities conducted in developing specific ICS component products, specific ICS integration and ICS operation:

- Support the establishment of minimal ICS security criteria applicable across control system industries.
- Support the establishment of minimal security criteria applicable to a single process control industry or single ICS installation.

It is envisioned that the applicability of this document and its derivatives to ICS industry security activities will grow over time. The information content and security capabilities

described in this document should be used to support each of the following aspects of the ICS life-cycle:

- Acquisition of ICS Products – There are two ways in which this document may serve the acquisition process:

1. Statement of required security capability – In this context, this document serves as the basis for communicating the minimal required security functionality that must exist in candidate products. The vendor community would incorporate a subset of the security capabilities defined by the specification as appropriate for the specific device(s) they manufacture.

2. Criteria to gauge sufficiency of available products – In this context the document serves as the basis for determining how close a candidate product comes to matching the required security capabilities.

- Verification of Compliance – There are two ways in which this document serves as a basis for determining the correctness of an implementation:

1. Evaluation at the component level – The evaluation would serve to substantiate the correctness of the implementation of a well-defined set of security functions and mechanisms.

2. Certification at the system level – The certification would serve to substantiate the correctness and suitability of the implementation for a well defined set of security functions within a well-defined operational environment and operational context.

In achieving any of the above goals it is important to recognize that a single security capabilities profile document can not be effective in addressing all the security issues and concerns of all US process control industries for each of the environments in which ICSs operate. Within each control industry, this document must be refined, tailored and elaborated with increasingly detailed information that is specific to the state, region, or industrial control facility within which the ICS is being employed. It is only at the ICS facility level that there can be details of the specific ICS components, architecture and day-to-day operational policies that govern the secure operations and maintenance of that ICS.

This concept for application of the document is illustrated in Figure 1 and parallels that taken when developing an enterprise-wide security policy. Corporate management will establish high-level policies that are applicable across all organizations within the corporation. Each corporate site, division, or other operational entity will then refine the high level policy into operational procedures. This process repeats and terminates at the lowest level of operation. It is at the lowest level operation that individual names, roles and other details specific to that operation can be stated with accuracy.

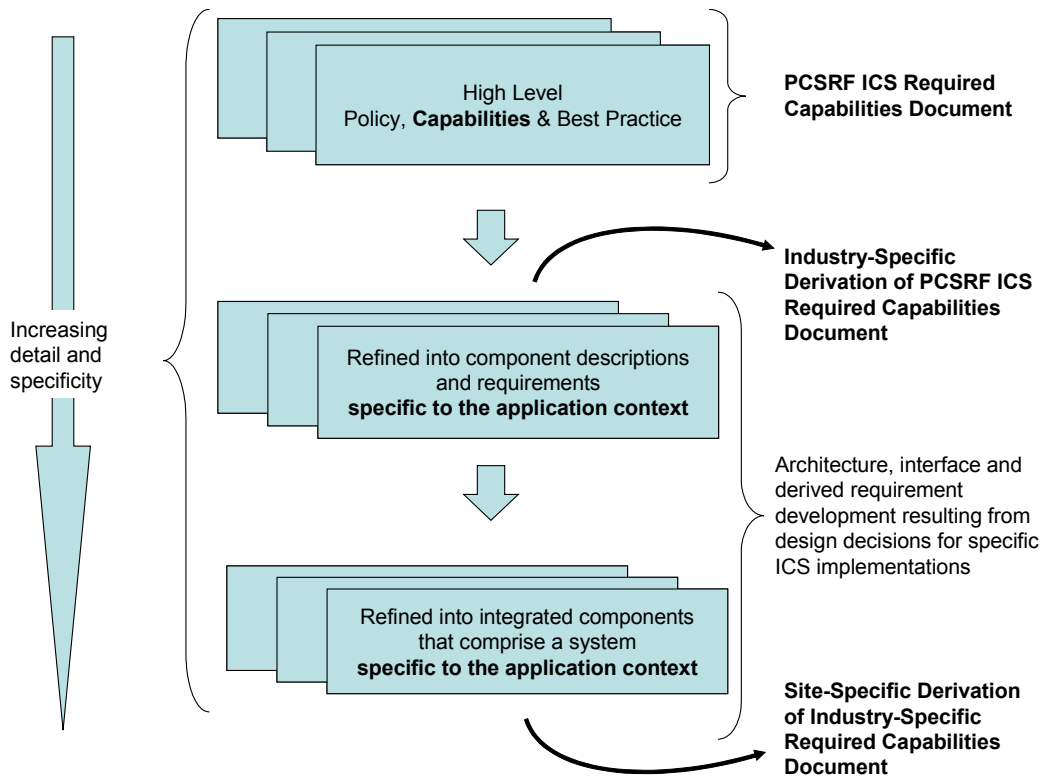


Figure 1 – Required Security Capabilities Document Refinement

### 1.5.3. Difference between Capability and Configuration

The terms capabilities and configuration, as used in reference to the engineering of systems are often used interchangeably although they have very different meanings. Capabilities refer to the *potential* for performing an action whereas configuration refers to a *specific instance* or *manner* in which the potential is put into effect.

As an example, a firewall may have the capability, or potential, to allow or disallow information to flow inbound to an organization's protected network from an external unprotected network. The firewall may also have the capability, or potential, to allow only authorized individuals to create, delete and modify the rules that determine the types of information flow that are allowed and disallowed. A specific firewall product will be designed, implemented and tested to demonstrate that it provides the desired capabilities. However, once that firewall is installed in an operational network it must be configured to enforce the specific details of an organizations' network information flow policy. Such a policy may require that only those individuals operating in the network administrator role be allowed to create, modify and delete information flow enforcement rules. That same policy might also require that all inbound information flows are restricted unless they are a response to an outbound information flow. It is necessary to have two types of documents: one to provide the statement of required capabilities and another to provide the statement of required operational configuration.



This document defines required capabilities but does not define any specific configuration of those capabilities in an operational context.

## 1.6. Relationship of this Document to other ICS Security Initiatives

Effective ICS security is implemented through application of comprehensive security-focused systems engineering, management, and operations and maintenance activities throughout the entire life-cycle of the ICS. This document focuses on security as it applies to a generic System Development Process as indicated in Figure 2. Figure 2 illustrated that this document is a receiver and provider of information and that there are concurrent security initiatives that provide information to or receive information from this document.

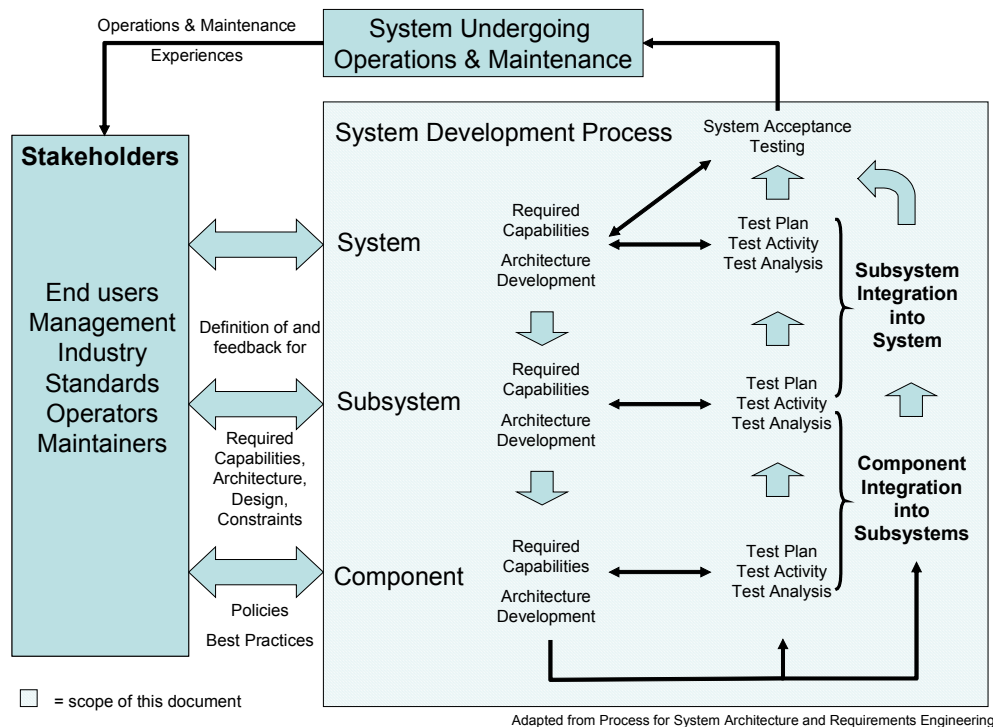


Figure 2 – System Life Cycle Activities

It is important to recognize that system development is an iterative process occurring simultaneously at several levels of abstraction: at the system level, at the subsystem level, and at the component or product level. This document defines ICS required capabilities independent of a specific architecture, at the ICS system level. The information in this document must be refined and tailored for each specific ICS in response to the details of the environment, the architecture, the subsystem definition and the components that comprise the subsystems.

### 1.6.1. Relationship with the PCSRF

The PCSRF provides the mechanism to facilitate information flow across control system sectors. This document and its protection profile derivatives are developed through the guidance and facilitation provided by the PCSRF.

#### 240    **1.6.2. Relationship with SP99**

The SP99 committee is working to establish an information base consisting of background security information, security technology surveys, and best security practices for instituting and maintaining a security program for ICSs, independent of specific industrial sectors. While the SP99 effort is broadly focused and comprehensive, it does not address  
245 the detailed security functional capabilities and security assurance measures that govern the design, development, verification and integration of ICS components.

The relationship between SP99 and this document is best described as follows: When the guidance and activities recommended by SP99 are put into effect for a *specific ICS*  
250 *operation*, the information generated can be used to refine and tailor this document and its derivatives into a security capabilities profile or security requirements specification for that specific ICS. Security products may be acquired, tested, integrated in to the ICS and the ICS itself may be verified to be compliant with the security capabilities profile or security requirements specification.

#### 255    **1.6.3. Relationship to NIAP & Common Criteria Recognition Arrangement (CCRA)**

From this document, Common Criteria-compliant Protection Profiles will be developed to foster development and evaluation of security products used to comprise ICSs. The protection profiles and developed products can be evaluated through oversight provided by NIAP.

260 NIAP is the US organization that operates a security product evaluation program that complies with international CCRA requirements. The CCRA provides the means for the results of security product evaluations to be recognized by all countries that participate in the CCRA. Through NIAP, a vendor may have a product evaluated in the US and have the  
265 results of that evaluation recognized in other countries. This minimizes the time, expense and resources required to demonstrate assurance in the security capabilities of a product for application in diverse operational environments. Likewise, the results of a security product evaluation performed outside the US by a country participating in the CCRA will be recognized by NIAP. Additional information on NIAP may be found at  
270 [www.niap.nist.gov](http://www.niap.nist.gov) and additional information on the CCRA and the participating countries may be found at [www.commoncriteria.org](http://www.commoncriteria.org).

#### **1.6.4. Relationship to industry-specific initiatives (e.g., CIDX, API, GTI, EPRI, NMCS)**

275 The various industrial control sectors each have initiatives targeted at defining sector-specific guidance and best practices for developing and operating security programs or for implementing security technologies into their ICSs. The relationship between the sector-specific initiatives and this document is very much like that of SP99 and this document: Where sector-specific efforts have developed detailed statements of security technology capabilities, that information may either be incorporated into a refinement of this  
280 document or referenced by the refinements of this document. Where sector-specific efforts have developed security program guidance and best practices for implementation within

their industry, the information collected from those actions can be used to develop refinements of this document.

### **1.7. Reading this Document**

285 Throughout the document there is explanatory discussion provided to aid the reader in  
understanding the material presented and in correlating the security-focused discussion  
into practical contexts. All such text is preceded by the header *Application Note* and is  
presented in an italicized font to distinguish the text from the main document text. The  
application notes can be broad in scope as they strive to address all stakeholder  
290 communities of interest: acquisition; vendors; integrators; operations and maintenance;  
test, evaluation and certification; policy and other mandate directorates, both governmental  
and industrial.

## 2. ICS System Definition and Description

This section defines the components of a control system in an abstract manner. The abstraction allows subsequent sections to discuss the security issues independent of the attributes specific to control system vendor products. This section does not address the security capabilities of systems that are external to the control system. Examples of these systems include enterprise management and office automation systems. This section does, however, address the security capabilities for the interfaces between the ICS and external systems.

An ICS is comprised of a collection of individual component types that are integrated together to manage an industrial production, transmission, or distribution process. These components may be categorized in terms of the fundamental function they provide within the ICS, such as a controller, sensor, transmitter or actuator. These components may also be characterized in terms of their basis of operation, which may be mechanical, pneumatic, hydraulic, electrical or electronic means. An additional categorization may be made when these fundamental functions are integrated together to provide multiple functions within a single physical housing, such as the combining of a sensor and transmitter function into a single physical unit.

The key control components of an industrial control system, including the control loop, the human machine interface (HMI), and remote diagnostics and maintenance utilities, are shown in Figure 1. A control loop consists of sensors for measurement, control hardware, process actuators, and communication of process variables. Measurement variables are transmitted to the controller from the process variable sensors. The controller interprets the signals and generates corresponding control signals that it transmits to the process actuators. This sequence of events results in new values of the process variables and the sensors transmit revised signals back to the controller. The human-machine interface allows a control engineer or operator to configure set points, control algorithms and parameters in the controller. The HMI also provides displays of process status information, including alarms and other means of notifying the operator of malfunctions. Diagnostic and maintenance tools often made available via modems and Internet enabled interfaces allow control engineers, operators and vendors to monitor and change controller, actuator, and sensor properties from remote locations. A typical ICS contains a proliferation of control loops, HMIs and remote diagnostics and maintenance tools integrated through an array of network protocols. Supervisory level loops and lower level loops operate continuously over the duration of a process at cycle times ranging on the order of minutes to milliseconds.

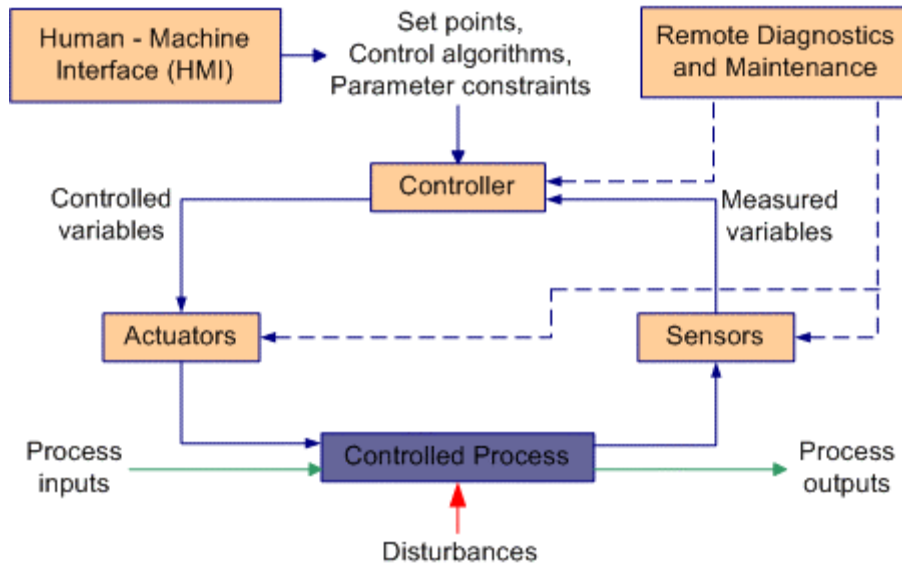


Figure 3 – Fundamental Control System Components

There are four primary commercially available industrial control system classifications. These include the programmable logic controller (PLC), the Distributed Control System (DCS), the Hybrid Control System (HCS), and the Supervisory Control and Data Acquisition System (SCADA). PLCs are highly scalable modular controllers with modules available for processing, discrete I/O, and analog input and output capabilities as well as communication interfaces. DCSs, HCSs and SCADAs are integrated systems that typically are configured to control a distributed process, where subsystems communicate over LAN, WAN, the Internet, Telephone Lines, and via Radio Frequency Transmissions depending on relative proximity of the subsystems. These distributed systems typically include a database historians and HMIs. DCSs and HCSs are similar, however HCSs are typically smaller systems and are tightly integrated by a single vendor and include a “built in” data historian, HMI and programming environment. Distributed systems that control processes that are distributed over large geographical areas are typically categorized as SCADA systems. A DCS, HCS, and SCADA system can contain several PLCs.

PLC’s are used to control discrete processes and are also used to control subsystems in DCS, HCS and SCADA systems. DCS and HCS are used to control large, complex processes such as power plants or refineries, typically at a single site. SCADA systems are used to control (perhaps) less complex, but more dispersed assets where centralized data acquisition is as important as control. Typically, distribution operations of water systems, gas pipelines, and electrical transmission lines use SCADA systems. Generic industrial control system network architectures are shown for both DCS and SCADA based control schemes in the Appendices. A glossary of terms describing the components found in the diagrams also can be found in the Appendix of this document.

Despite the different nomenclature, the underlying concepts, components, and functions of PLC, DCS, HCS and SCADA systems are similar. Therefore, this document targets the ICS in an abstract sense – it might be on of the systems described above, or some

365 combination of these or other configurations. The ICS is characterized by components that  
record information, monitor information, transmit information, receive information or  
determine and issue command sequences.

### 3. Operational Security Environment

The security environment establishes the context in which the ICS operates. It is described in terms of technical controls and administrative controls. The technical controls are technology-based (i.e., the computer and communications hardware, software and firmware) while administrative controls are non-technology-based (i.e., physical controls, personnel, policies and procedures). The discussion is presented primarily in terms of assumptions, vulnerabilities, regulatory mandates and policies as they relate to the security environment.

- Assumptions – The assumptions regarding the intended operational environment serve to bound the problem space and problem definition. They are expressed relative to the physical and computer operating environment, the technology employed in control systems and the common and unique aspects of the varying process control industries that will make use of this specification.
- Vulnerabilities – Statement of vulnerabilities are made within the context of the stated assumptions. Vulnerabilities apply to the control system as well as to the systems to which the control system interfaces and the physical procedures that govern the use of the control system.
- Regulatory Mandates & Policy – Mandates, policies or directives that govern the use and application of control systems are stated since they may require mechanisms to support the enforcement of the criteria. The scope of relevant regulatory constraints should be consistent with the stated vulnerabilities.

#### 3.1. Secure Usage and Environment Assumptions

Assumptions are presented with respect to the intended use of the ICS and the operational environment in which the ICS shall be used. Each assumption has a label of the form “A.<unique-name>” to aid in supporting traceability. Assumptions are axiomatic, that is, they state a condition that is to exist in the environment of the implemented ICS. Therefore, each assumption must be qualified against each individual ICS.

##### A.External\_System\_Capability

The scope of this document is limited to what is defined as the ICS. The security capabilities of systems or components external to the ICS definition are not stated in this document.

*Application Note: Experience has been that the precise boundaries of the ICS are not always easy to establish. For example, if you have a supervisory or multi-variable control application driving setpoints to the controllers, is this part of the ICS scope? One approach that we have used to establish this boundary is to say that any element that can **directly** impact the safe and reliable operation of the process is considered within scope. Using this definition, systems such as MVC's*

would not qualify, since they only “request” changes that must then be validated and implemented at the control level (i.e., setpoints).

#### A.External\_System\_Interface

The scope of this document includes the security behavior at and across the interfaces and interconnects between the ICS and external systems.

*Application Note: An interface is the boundary between two communicating entities (e.g., socket, API, RPC). An interconnect is the medium over which or means by which communication occurs (e.g., wire, wireless, leased line, Internet, etc, to include protocols (e.g., TCP/IP, FieldBus, ICS proprietary protocol).*

#### A.Control\_System\_Physical\_Access

An individual that is granted access within the ICS facility will have physical access to ICS components located within the ICS facility.

*Application Note: We are assuming that authorization to be in the facility implies that opportunity exists to access the control system. Such access may be possible via direct interaction to control system components or via indirect access via the facility network infrastructure.*

*Application Note: Realize that this assumption may be true only in some cases within a facility. For example, can we make a distinction between the control room and other locations within the facility where control system components reside?*

*Application Note: This assumption is not intended to imply that an individual who is granted physical access to an area in which a control system component resides is also granted access to the control system and is granted access to use the control system. Perhaps a rewording would be appropriate to clarify the intent of this assumption.*

*Application Note: DOW has defined a logical concept called the “Operating Area” which is defined as including any physical location from which operations tasks or commands may originate. Typically, this is synonymous with the control room, but with things like wireless control devices and roving operators, this may not always be the case. Another example would be a remote product loading station. The logical sum of that location and the control room would constitute the “Operating Area”.*

#### A.ICS\_External\_Network\_Connectivity

The ICS network may have connectivity with non-ICS system networks through which Internet connectivity is possible.

*Application Note: The implication is that the control system may be accessed via an external internet connection and that internal access to the control system is possible from other facility networks.*

#### A.Remote\_Access




Remote access to ICS components may be available to authorized individuals.

460 *Application Note: Authorized individuals include product vendors, integrators, maintainers as well as personnel employed at the process control facility.*

#### A.Physical\_Security\_Sophistication


465 The degree of physical protection provided to control system components, excluding communication medium, is largely a function of the criticality of the specific process being controlled, and plant circumstances to include the physical location of the control system components.

#### 470 A.Boundary\_Defense

 ICS operations facility will have effective protection mechanisms in place to control access to the ICS from a device not located on the ICS network.

475 *Application Note: If the ICS definition includes the referenced protection mechanisms, then this assumption is invalidated and should be removed*

#### A.Accessible\_Comm\_Medium

480  There is no physical protection of the ICS communication medium.

*Application Note: Recommend delete.*

#### A.No\_Infrastructure\_Security\_Services

485 There are no security services provided by the communications infrastructure for the ICS components.

490 *Application Note: There are no expectations for communication mediums to be secure. There are also no expectations that any security may be derived from components that implement the communications infrastructure.*

### 3.2. Vulnerabilities

495 The statement of vulnerabilities establishes a basis for the derivation of specific security capabilities to be implemented by the ICS. ICS vulnerabilities have been derived from PCSRF meetings and ICS sector-specific workshops. Each statement of vulnerability has relevance to at least one of the following contexts:

- Intended operational environment of the ICS components;
- Purpose, function and use of the ICS components;
- 500 • Technology employed in ICS components;
- Communication medium employed to provide connectivity between ICS components;

- Human agents with intent to disrupt, destroy or incapacitate ICS operation;
- Natural disaster events that can disrupt or destroy or ICS operation.

505

The following statements provide a characterization of the vulnerabilities that may be exploited for the intent of disrupting or otherwise preventing a ICS from accomplishing its designed intent. Each vulnerability has a label of the form “V.<unique-name>” to support traceability to specific objectives and capabilities.

510

#### V.Intercept-Analysis

- Information flows between ICS components are subject to interception and analysis.

515

#### V.Intercept-Replay

- Information flows between ICS components are subject to interception and replay.

520

#### V.Intercept-Modify

- Information flows between ICS components are subject to interception and modification and replacement.

525

#### V.Inserted-Information-Flow

- Information flows between ICS components may be inserted.

#### V.Unauthorized-Upload

530

- Unauthorized executable code may be uploaded to an ICS component.

#### V.Fault-Detection

535

- An ICS component with responsibility for supervisory or control functionality is unable to detect actual ICS component failure or to detect an ICS degraded mode of operation.

#### V.Safety-Critical

540

- ICS components providing secure supervisory or direct control functionality have a failure mode with safety-critical implications.

545

*Application Note: Recommendations both to keep and delete. The issue is this: if the concepts of “secure failure mode” and “recovery from a secure failure mode” are to be built into the ICS, there must be a justification for having that capability. The justification does not necessarily have to be made in terms of the safety angle; however, the safety angle provides a compelling case for the functionality.*

### 3.3. Regulatory Mandates & Policy

550 Regulatory mandates and policy statements are the basis for stating capabilities that must be implemented by the ICS. These capabilities are constraints imposed on ICS operations by governmental, industry-specific or other entities with jurisdiction over the control industry and its ICS operations. Each policy has a label of the form “P.<unique-name>” to aid in supporting traceability.

555 This polices in this section should have overlap and consistency with related control system industry security initiatives that provide, establish or recommend best practices, policies and procedures for secure ICS operations (e.g., SP99).

#### P.Safety\_Dependency

560

ICS security capabilities shall be implemented to include securing the interfaces and interconnects of the ICS safety systems.

#### P.Operational\_Non\_Interference

565

ICS security capabilities shall be implemented to not impede the nominal operation of the ICS and to not impede the safety systems that protect the ICS.



570

*Application Note: The interpretation of the term “nominal” varies for different ICS sectors and varies within a single ICS implementation. Nominal includes, but is not limited to, real-time constraints (e.g., handling interrupts), bandwidth constraints and resource constraints (e.g., processor or memory).*

#### P.Risk\_Assessment

575

The ICS shall be designed, implemented, and operated to meet the risk objectives resulting from a system life-cycle risk management program. The risk management program shall establish a comprehensive and integrated set of risk management goals for issues affecting ICS operation, ICS safety and ICS security.

580

#### P.Business\_Continuity

585 The ICS shall be operated in accordance with a business continuity policy that addresses the identification of and response to events that adversely affect the ability of the ICS to operate in fulfilling its design goals.

## 4. Industrial Control System Capability Objectives

This section documents the capability objectives that must be met by a compliant ICS. The capability objectives apply to both the technology-based components of the ICS and to the non-technology physical controls, personnel and procedures of the ICS.

### 590 4.1. ICS Non-Technical Operations Objectives

Each operations objective has a label of the form “OO.<unique-name>” to aid in supporting traceability.

#### OO.Business\_Continuity

595

The ICS shall be operated in accordance with a business continuity policy that addresses the identification of and response to events that adversely affect the ability of the ICS to operate in fulfilling its design goals.

600 *Application Note: The policy should address knowing what can happen, what the implications are when something happens, and what to do when those events happen. The policy is likely to focus on availability issues.*

#### OO.Regulatory\_Compliance

605

The control system shall be operated in compliance with relevant governing mandates.

610 *Application Note: The issue of ensuring compliance with regulatory mandates requires identification of such mandates and the assessment of how to incorporate the appropriate language in the requirements spec to ensure that such compliance may be demonstrated.*

#### OO.Risk\_Assessment

ICS risk assessments shall be conducted such that:

615

- The control system general operating environment and application of security technology is periodically updated,
- The results of the risk assessment are relevant to and are applied throughout the control system life cycle process,
- 620 • A documented and approved risk assessment process is followed.

*Application Note: Risk assessment activity must be done on a periodic basis and the results utilized throughout the system development and operational life-cycles.*

#### 625 OO.Security\_System\_Verification

The control system components and control system as an integrated unit shall undergo verification analysis and testing to ensure that the control system

- 630
- Meets its design specification
  - Is properly installed and integrated
  - Is properly configured per operational policies

#### OO.Migration\_Strategy

635

A migration strategy shall be developed to govern the evolution of the control system throughout its operational life-cycle. The migration strategy shall address at a minimum:

- 640
- Definition and continuous maintenance of the current system state (components, configuration, etc).
  - The integration between computer implemented and personnel implemented procedures.

645 A verification plan shall be developed to ensure that the migration strategy is being executed properly that the migration strategy is accurately defined

The migration strategy shall be refined in response to findings during the execution of the verification plan.

#### 650 OO.Collaborative\_Working\_Relationships

Policies governing the roles, responsibilities and activities authorized for individuals not employed by the control system operating organization shall be developed.

655 The policies shall establish methods for on-site internal, on-site remote and off-site remote access to control system resources.

*Application Note: There is need for well-defined rules governing the interaction with business partners of the ICS organization and the action taken should the rules be violated.*

660

#### OO.Security\_Ownership

A policy governing security shall be defined to establish the following:

- 665
- an organization-wide security management infrastructure
  - identified roles with authority and responsibility to operate within the infrastructure

670 The policy shall define a single office with responsibility for the security of all control system and non-control system computer resources and the personnel authorized to manage those resources.

*Application Note: There is a need for a single authority with responsibility for all ICS operations, and to remove the top-level distinction between control and IT systems.*

## 4.2. ICS Technology-Based Objectives

675 The following ICS technology-based objectives establish the high-level statement of functional security capabilities that are to be met through combinations of hardware, software and firmware. Each objective has a label of the form “TO.<unique-name>” to aid in supporting traceability.

680 TO.Non\_Interference

The control system security functions shall be implemented in a non-interference manner such that behavior of the primary control system functions and safety functions are able to meet their performance constraints.

685

TO.Security\_Override

The control system shall provide the capability for the controlled bypass of security mechanisms in those instances where security policy enforcement conflicts with the continued safe operation of the control system.

690

*Application Note: This objective requires that designed over-ride mechanisms be in place to ensure that a safety-critical state is not created or an existing safety-critical state is not worsened due to security protection mechanisms.*

695

*The “controlled bypass” aspect of the objective means that the security policy includes the ability to override the security enforcement mechanism. When possible, the specific details regarding the bounds and conditions for the override capability should be stated.*

700 TO.Access\_Control

The control system shall provide the capability to grant or deny access to control system resources based upon the authorizations associated with authorized subjects.

705 *Application Note: A subject is an individual or role, or a process acting on behalf of an individual or role.*

The control system shall deny unauthorized agents access to every control system resource.

710

The control system shall require that each agent authorized to use the control system is identified and is provided with credentials to authenticate their identity.

715 The control system must be able to include knowledge of the control system state and/or the controlled process state when making an access control decision.

The control system shall include knowledge of time and location in the rules for making an access control decision.

720 TO.Communications\_Integrity

The control system shall provide the capability to allow information flows only between authenticated and authorized endpoints.

725 The control system shall provide the capability to protect information flows from replay, substitution or modification.

The control system shall provide the capability to allow the recipient of an authorized information flow to verify the correctness of the received information.

730

TO.Control\_System\_Integrity

The control system shall provide the capability to restrict access to the functions used to establish and maintain the secure operational configuration of the control system.

735

The control system shall be capable of performing self-tests to verify the configuration and integrity of the security functions of the control system.

740 The control system shall provide the capability for self-test to be executed on startup, at periodic intervals, and on demand.

The control system shall be capable of responding to integrity failures.

745 *Application Note: This is left abstract as the response may be as simple as illuminating an indicator or sending a message. Or the response may be as complex as automatically taking corrective action to contain the failure (fail secure or reconfigure for degraded mode operation).*

TO.Event\_Trace

750

The control system shall provide the capability to record and maintain event traces that reflect the successful and unsuccessful security relevant activities involving control system resources.

755 *Application Note: The specific discussion focused on audit and there are some considerations that must be addressed, such as, what does audit mean in a control system context (i.e., what type of activity and what types of events are recorded) there were no unique issues brought up. This issue is closely related to the Control Systems Intrusion Detection System (CIDS) issue since the detection capability might utilize event traces as a means to detect potential policy violations.*

760

TO.Intrusion\_Detection

The control system shall be capable of detecting unauthorized activity, unusual activity and attempts to defeat the security mechanisms of the ICS.

765

*Application Note* The ICS security policies establish the basis for what is considered 1) authorized, 2) usual and 3) that result in enabling and configuring security mechanisms. Therefore, this objective is tied directly to the defined policies enforced by the ICS.

770 The control system shall be capable of initiating action in response to the detection of a potential violation of a nominal use control system policy.

*Application Note:* There was discussion regarding need for proactive response to an attack. Proactive response to an attack is considered as meaning automatic response to an attack, that is, without human intervention. The need for capabilities to monitor activity on the control network and to detect activity that is beyond 'nominal' requires 'nominal' must be defined. By defining the norm a policy may then be established and only then will it be possible to detect potential violations of policy (i.e., an intrusion). The next step would be to define policy for the response to the potential intrusion.

780 TO.Operational\_Configuration\_Integrity

The control system shall provide the capability to determine the current configuration of a control system component.

785 The control system shall provide the capability for a controlled update to the current configuration of a control system component.

790 The control system shall provide the capability to restrict the use of the controlled update function.



## 5. Control System Component Security Capability Requirements

This section documents the requirements to be met by the ICS. The requirements are grouped as they might apply to the entire ICS, to an ICS subsystem or to one or more ICS components. The scope of the requirements fall into the following categories:

- Documentation
- Configuration Management
- Access Control
- Integrity
- Functional Security Testing
- Penetration Testing, Vulnerability and Risk Assessment

### 5.1. Security Functional Implementation Requirements

#### 5.1.1. ICS Security-Related Event Recording and Auditing

- a. The ICS shall provide a capability to record security relevant events.
- b. Each recorded event shall include the following information to support post-event analysis or reconstruction of ICS activity.
  - i. Event timestamp (date and time)
  - ii. Event description
  - iii. Verdict depicting result of the event (e.g., success, failure)
  - iv. Identity of participant(s) in the event (e.g., device, individual, role)
  - v. Event-specific explanatory information
- c. The ICS shall provide semi-automated or fully automated capabilities to review the event audit trail for identification of potential security policy violations.
- d. The ICS shall provide semi-automated or fully automated capabilities to send a notification for each potential security violation as follows:
  - i. For a set of security violations, the alarm shall be immediate
  - ii. For a set of security violations, the alarm shall be verified prior to the notification being made
- e. The ICS shall provide the capability to manage the behavior of the event generation and recording capabilities
  - i. Startup, shutdown, backup, recovery
  - ii. Selection of events to audit based upon attributes specific to the events to be recorded
  - iii. Searching of events based upon attributes specific to the recorded events

- 830 f. The ability to modify the behavior of the event generation and recording capability shall be restricted to authorized individuals.

### 5.1.2. Communication Channels and Interconnects

- 835 a. A secure channel between communicating devices shall be established prior to any information being passed between device pairs.
- b. The secure channel shall be defined as follows:
- i. Each endpoint of the communication shall authenticate the other endpoint
  - 840 ii. Information flow between the authenticated endpoints shall occur in accordance with specific rules defined for that secure channel.
- c. The information flow rules shall address
- i. Data content type, form and attribute values
  - 845 ii. Flow direction and conditions for authorized flows
- d. The secure channel shall be maintained to ensure:
- i. each endpoint shall accept information received from an authenticated endpoint that is authorized to transmit the received information
  - 850 ii. each endpoint shall reject information received from
    - i. a device that is not authenticated
    - ii. a device that is not authorized to transmit the received information
  - iii. Loss of connectivity results in attempts to reestablish the secure channel
  - iv. Endpoints shall detect and reject incorrectly formed and erroneous data
  - v. Endpoints shall detect and reject data that is inserted without
  - 855 authorization
  - vi. Endpoints shall detect and reject data that is modified without authorization
  - vii. Endpoints shall institute recovery action when incorrectly formed or erroneous data is received
  - 860 viii. The behavior of the secure channel shall be managed by authorized individuals
  - ix. Each device shall authenticate the individual attempting to modify the behavior of the device prior to acting on any behavior change commanded by that individual
  - 865 x. Each device shall be capable of accepting only legitimate commands and command attribute values

### 5.1.3. Boundary Defense Devices

- a. A boundary defense device shall be capable of controlling the flow of information across its external interfaces.
- 870

- b. The boundary defense device shall be capable of explicitly allowing or explicitly denying information flow based on a set of rules that address
  - i. The type of information (e.g., command action, status request, configuration request)
  - 875 ii. The source identity of the information (device, individual)
  - iii. The destination identity for the information (device, individual)
  - iv. The protocol used
  - v. The communication channel or port through which the information passes
  - 880 vi. The time of day
  - vii. [other parameters]
- c. The boundary device shall be capable of generating events associated with the flow of information across its interfaces
  - 885 i. Each generated event shall include the disposition of the information flow
  - ii. Each generated event shall include attributes of the information flow
- d. The behavior specified by the information flow rules shall be managed by authorized individuals
  - 890 i. The boundary device shall authenticate the individual attempting to modify the information flow rules prior to accepting any modifications to the rules
  - ii. The boundary device shall record the actions of the authorized individual who modifies the information flow rules
  - 895 iii. The boundary device shall be capable of accepting only legitimate commands and command attribute values

900 *Application Notes: A boundary defense device is a device that establishes a point of separation between two or more interconnected networks. The boundary device provides functions to monitor and control the flow of information (operational, maintenance, command) between the networks.*

#### **5.1.4. Network Addressable Field Devices**

- a. The network addressable field device shall be capable of identifying and authenticating itself to devices it interfaces with.
- 905 b. The network addressable field device shall be capable of responding to operational, performance and maintenance commands provided by or from an external device.
  - i. The network addressable field device shall accept control system operational, performance and maintenance commands from authenticated sources
  - 910 ii. The network addressable field device shall reject control system operational, performance and maintenance commands from sources that cannot be authenticated
  - iii. The network addressable field device shall be capable of qualifying each command prior to performing the commanded action

- 915                    i. A command shall be rejected if it places the device in an unsafe state
- ii. A command shall be rejected if it places the device in a non-secure state

920                    *Application Note: An unknown state may be treated as either an unsafe or non-secure state.*

- c. The network addressable field device shall be able to verify the integrity of its operational hardware, software and firmware base.
- 925                    d. The network addressable field device shall be able to detect potential violations of the security policy that it enforces.

*Application Note:*  
*This requirement is not applied as an absolute such that every aspect of the security policy being enforced is also a candidate for determination of a potential violation.*

930

- e. The network addressable field device shall be able to determine that it has been initialized into a secure operational state prior to accepting control system operational, performance, or maintenance commands.
- 935                    f. The network addressable field device shall be capable of failing into a secure state.

*Application Note: The secure state may allow for continued operation albeit in a degraded or reduced capability mode. The secure state may result in cessation of all processing and communication capability, effectively resulting in a “fail-stop” halt condition.*

940

- g. The network addressable field device shall be capable of recovering from a failed secure state to an operational secure state.

945                    *Application Note: Operational secure state may be a maintenance state or a control system operational state.*

- h. For first time initialization, the network addressable field device shall initialize into a limited capability secure state.
- 950                        i. The network addressable field device shall require the selection and use of non-default authentication credentials;
- ii. The network addressable field device shall require explicit authorization prior to establishing communication with other devices.

955                    *Application Note: The definition of limited must be provided for each device type to which the requirement applies.*

#### **5.1.5. Control System Operator Command Console**

- a. The control system operator command console device (console device) shall be capable of authenticating individual ICS operators based on each of the following or combinations of the following attributes:
- 960

- i. Unique individual identity
  - ii. Role independent of individual identity
  - iii. Role associated with individual identity
- 965 b. The console device shall maintain capabilities that are associated with individuals or associated with roles.
- c. The console device shall allow an individual to have authorizations for multiple roles.
- d. The console device shall provide the capability to prevent an individual from obtaining multiple roles simultaneously.
- 970 e. The console device shall provide the capability to require an individual to explicitly request a change in role.
- f. The console device shall provide the capability for role or authorization restrictions to be overridden.
  - i. The use of the override capability shall be recorded.
  - 975 ii. The override capability shall have a configurable time span after which the previously established authorizations shall be reinstated.
- g. The console device shall be capable of protecting an authorized control session from unauthorized use
  - i. The console device shall provide a configurable capability to lock the active session
    - 980 1. Mandatory session locking shall occur when the configured time of inactivity is exceeded.
    - 2. Operator-defined session locking shall occur by explicit operator action
  - 985 ii. The console device shall provide the capability for re-authentication of the individual
  - iii. Re-authentication shall be required prior to issuing a set of commands
  - iv. Re-authentication shall be required prior to accessing specific information
  - 990 v. Authentication and re-authentication shall be implemented with an appropriate strength mechanism.
  - vi. Single factor authentication based upon a user id and password or user id and PIN shall require
    - 1. Minimum character length for passwords and minimum number of digits for PIN sequences
    - 995 2. The use of combinations of upper and lower case alpha characters and punctuation/special characters for passwords
  - vii. Two-factor authentication employing challenge-response or on-time-password hardware tokens shall have an appropriately sized pseudo-random number generator
  - 1000 viii. Two-factor authentication employing encryption technology shall
    - 1. employ encryption key lengths of sufficient length to provide the required strength for the encryption algorithm used
    - 2. employ certified encryption algorithms

1005 *Application Note: While the strength of a specific encryption algorithm/key length combination may be quantified, the concept of an “appropriately strong”*

*algorithm/key length combination for a specific application context is subjective. The intent of the requirement is to ensure that thought is given to the selection of the encryption mechanism and for there to be evidence that supports that selection.*

1010

- ix. Two-factor authentication employing biometric technology shall provide the capability for configuration of the false acceptance rate and false rejection rate parameters.

1015

- h. The console device shall be capable of failing into a secure state.
- i. The console device shall be capable of recovering from a failed secure state to an operational secure state.

1020

- j. The console device shall be capable of operating in a degraded mode.

*Application Note: The degraded mode definition and characteristics must be defined.*

1025

- k. The console device shall provide the capability for device fail-over or device function fail-over.

## **5.2. Security Verification, Operation and Maintenance Assurance Requirements**

### **5.2.1. ICS Policy Documentation**

- a. ICS operational policies shall be developed and maintained.
- 1030 b. The ICS operational policies shall address
  - i. ICS roles, responsibilities and authority regarding ICS management, operations, administration and maintenance
  - ii. ICS intended usage and compliance with operations procedures
  - 1035 iii. Agreements between ICS management and the management of external systems or devices to which the ICS receives or transmits information

### **5.2.2. Architecture Documentation**

- a. The ICS architecture shall be documented and maintained.
- 1040 b. The ICS architecture documentation shall include:
  - i. Physical layout of network
  - ii. Definition of ICS subsystems and protection domains
  - iii. Placement of ICS components in the network
  - iv. Logical flows of information between ICS subsystems and components through the network
  - 1045 v. Definition of interfaces and interconnects
    - 1) As they apply externally to ICS components
    - 2) As they apply externally and internally to ICS subsystems

- 3) As they apply externally to the ICS to enable integration with other systems or devices

1050

### **5.2.3. Configuration Documentation**

- a. The operational configuration of ICS components shall be documented and maintained.
- 1055 b. The ICS operational configuration documentation shall include:
  - vi. Component version number(s)
  - vii. Unique identification of applied patches or service packs
  - viii. Installation, startup, steady-state runtime, and shutdown parameters

### **5.2.4. Design Documentation**

- 1060 a. The design of ICS components shall be provided for use by ICS system integrators.
- b. The component design documentation shall include:
  - i. Definition of external interfaces
  - 1065 ii. Description of behavior or functionality provided at the interface
  - iii. Description of fault and error conditions
  - iv. Description of secure startup and shutdown procedures
  - v. Description of secure hardware, firmware or software update procedures
  - vi. Description of component secure failure and secure recovery operation
  - 1070 vii. Guidance governing secure installation of the component
  - viii. Guidance governing secure integration of the component into the ICS
  - ix. Guidance governing secure operation of the component
  - x. Guidance governing secure maintenance of the component

### **5.2.5. System Testing**

- 1075 a. The ICS components shall be integrated and tested prior to their use to support operational control system functions.
- b. An ICS test plan shall be developed and maintained.
- 1080 c. The ICS test plan shall include the following:
  - i. ICS integration test strategy
  - ii. ICS component installation verification test procedures
  - iii. ICS subsystem integration and verification test procedures
  - iv. ICS system verification test procedures
  - 1085 v. ICS interoperability with external devices test procedures
- d. The test procedures shall include:
  - i. Testing sequence dependencies

- 1090                    ii. Configuration verification
- iii. Expected and actual test results

#### **5.2.6. Residual Risk Assessment**

- a. The ICS shall undergo periodic assessment to determine the level of residual risk.
- 1095                    b. The periodic assessments shall include
  - i. Verification of correct configuration
  - ii. Determination of new vulnerabilities
  - iii. Penetration testing to intentionally defeat the security countermeasures



## 6. Appendix I – Process Control Systems and Industries Overview

1100 Real-time computer control systems used in process control applications have many characteristics that are different than traditional information processing systems used in business applications. Foremost among these is design for efficiency and time-critical response. Security is historically not a strong design driver and therefore tends to be bypassed in favor of performance. Computing resources (including CPU time and memory) available to perform security functions tend to be very limited. Furthermore, the goals of safety and security sometimes conflict in the design and operation of control systems.

1110 Digital industrial control systems can be either process-based or discrete-based. Process-based controls are used to control continuous processes such as fuel or steam flow in a power plant or petroleum in a refinery. Discrete-based controls (otherwise known as batch controls) control discrete parts manufacturing or “batches” of material in a chemical plant. Both utilize the same types of control systems, sensors, and networks. While efforts of the PCSRF are currently geared toward continuous processing systems, results will likely be applicable to discrete based systems.

1115 The computer control systems used in process industries, including electric utilities, petroleum (oil & gas), water, waste, chemicals, pharmaceuticals, pulp & paper, and metals & mining can be divided amongst the usage of either DCS or SCADA technology and implementation depends on the geographic distribution of the operation. Network architectures that encompass processing operations involving the transformation of raw materials into a usable product in a continuous fashion follow the DCS scenario. On the other hand, the network architectures that encompass distribution operations of the usable products, typically over large distances, follow the SCADA scenario.

1125 The electrical power infrastructure is made up of power generation facilities as well as transmission and distribution networks (electric power grid) that create and supply electricity to end-users. Power generation facilities include both fossil fuel and hydroelectric systems. Fossil fuel plants use a combustion process to heat water in a boiler to steam. The high-pressure steam, in turn, flows into a turbine, which spins a generator to produce electricity. Hydroelectric generation facilities utilize the force of water, via a dam, flowing into a turbine, which spins a generator to produce electricity. These generation facilities use DCS. The electric power grid is a highly interconnected and dynamic system consisting of thousands of public and private utilities and rural cooperatives. A SCADA system manages distribution systems by collecting the electric system data from the field and issuing control commands to the field.

1140 Natural gas, crude, refined petroleum, and petroleum-derived fuels represent Oil and Gas substances. The Oil & Gas infrastructure includes the production holding facilities, refining and processing facilities, and distribution mechanisms (including pipelines, ships, trucks, and rail systems) for such substances. Refining and processing facilities make use of DCS while holding facilities and distribution systems utilize SCADA technology.

The water supply infrastructure encompasses water sources, holding facilities, filtration, cleaning and treatment systems and distribution systems. Like electric, oil and gas, the processing operations use DCS technology while the distribution operations use SCADA technology. A wastewater treatment infrastructure is very similar to that of a water supply infrastructure. Chemical, pharmaceutical, pulp and paper, and metals and mining industries primarily fit into the category of processing facility and use DCS technology.

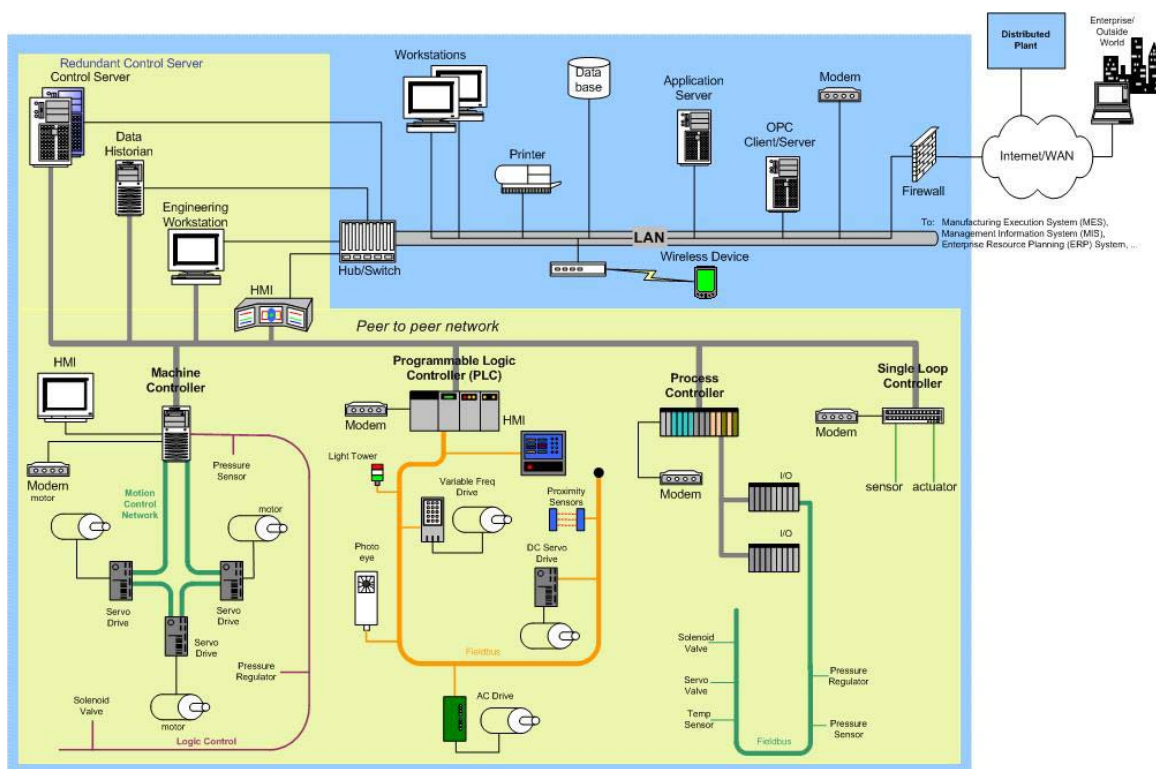
A comparison of these diagrams shows that at the higher level of the plant network architectures the plant operations are similar for plants containing either DCS or SCADA systems. At this level, everything resides on a local area network. These include general-purpose workstations, printers, plant database, application servers and domain controllers. Communication outside the plant is typically established via a firewall to the Internet or a wide area network (WAN). Modems are also available, usually to allow remote access to employees working from home or on the road. The DCS and local SCADA components of a plant system typically reside on a peer-to-peer network.

### **6.1. DCS Component Characterization**

A DCS is comprised of a supervisory layer of control and one to several distributed controllers contained within the same processing plant. The supervisory controller runs on the control server and communicates to its subordinates via a local network. The supervisor sends set points to and requests data from the distributed controllers. The distributed controllers control their process actuators based on requests from the supervisor and sensor feedback for process sensors. These controllers typically use a local field bus to communicate with actuators and sensors eliminating the need of point-to-point wiring between the controller and each device. There are several types of controllers used at the distributed control points of a DCS including machine controllers, programmable logic controllers, process controllers and single loop controllers depending on the application. Many of the distributed controllers on a DCS have the capability to be accessed directly via a modem allowing remote diagnostics and servicing by vendors as well as plant engineers.

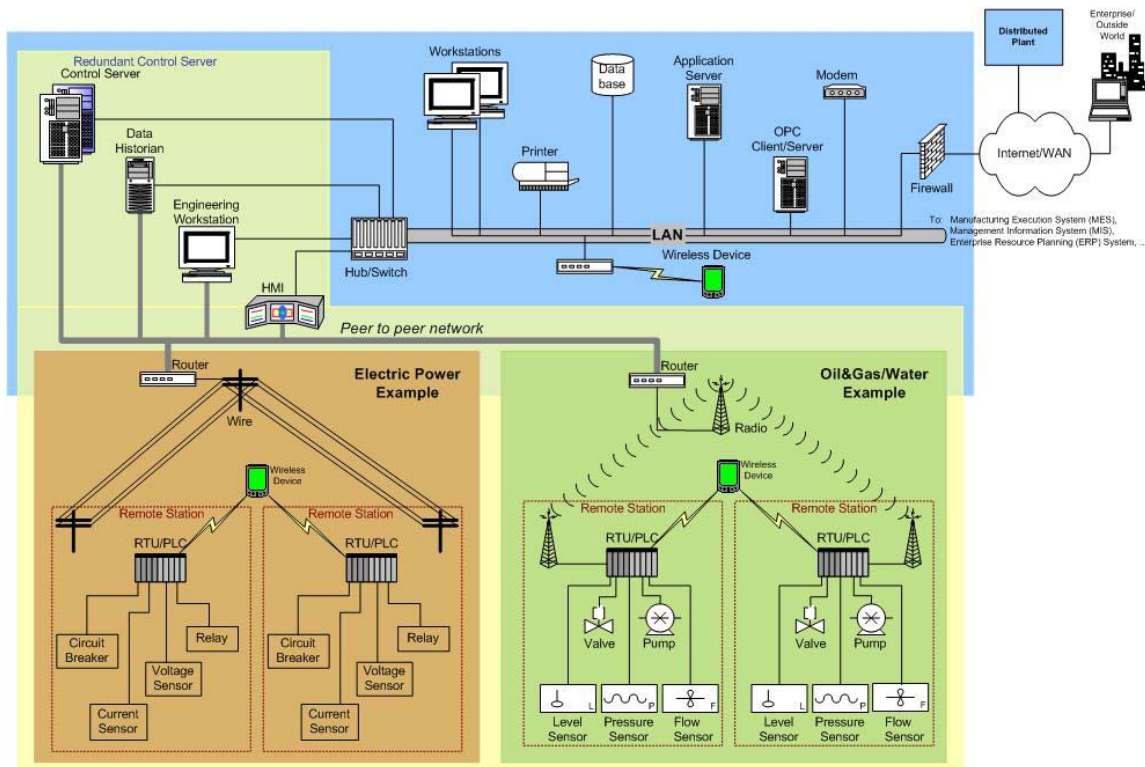
### **6.2. SCADA Component Characterization**

A SCADA typically consists of a Central Monitoring System (CMS), contained within the plant and one or more Remote Stations. The CMS houses the Control Server and the communications routers via a local network. The CMS collects and logs information gathered by the remote stations and generates necessary actions for events detected. A remote station consists of either a Remote Terminal Unit (RTU) or a Programmable Logic Controller (PLC) that controls actuators and monitors sensors. Remote stations, typically, have the added capability to be interfaced by field operators via hand held devices to perform diagnostic and repair operations locally. The communications network is the medium for transporting information between remote stations and the CMS. This is performed using telephone line, cable, or radio frequency. If the remote site is too isolated to be reached directly via a direct radio signal, a radio repeater is used to link the site.



1185

Generic Industrial Control System Network Architecture - DCS



Generic Industrial Control System Network Architecture - SCADA

## **7. Appendix II – Glossary of Terms – Generic Composite Industrial Control System Network Architecture**

1190

AC Drive – Alternating Current Drive synonymous with Variable Frequency Drive (VFD).

Application Server – A computer responsible for hosting applications accessed and used by multiple networked user workstations.

1195

Control Server – A server hosts the supervisory control system, typically a commercially available application for DCS or SCADA systems.

1200

DataBase – A repository of information that usually holds plant wide information including process data, recipes, personnel data and financial data.

DC Servo Drive – A type of drive that works specifically with servo motors. Transmits commands to the motor and receives feedback from the servo motor's resolver or encoder.

1205

Distributed Control System (DCS) – A supervisory control system typically controls and monitors set points to sub-controllers distributed geographically throughout a factory.

Distributed Plant – A geographically distributed factory that is accessible through the Internet by an enterprise.

1210

Enterprise – A business venture or company that encompasses one or more factories.

1215

Enterprise Resource Planning (ERP) System – A system that integrates enterprise-wide information including human resources, financials, manufacturing, and distribution as well as connect the organization to its customers and suppliers.

1220

Fieldbus - A category of network that links sensors and other devices to a PC or PLC based controller. Use of Fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network.

Firewall – A device on a communications network that can be programmed to filter information based on the protocol, source or destination.

1225

Human Machine Interface (HMI) – The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.

1230

Internet – a system of linked networks that are worldwide in scope and facilitate data communication services. The Internet is currently a communications highway for millions of users.

- 1235 Input/Output (I/O) – a module relaying information sent to the processor from connected devices (input) and to the connected devices from the processor (output).
- Light Tower – A device containing series of indicator lights and an embedded controller used to indicate the state of a process based on an input signal.
- 1240 Local Area Network (LAN) – A network of computers that span a relatively small space. Each computer on the network is called a node, has its own hardware and runs its own programs, but can also access any other data or devices connected to the LAN. Printers, modems and other devices can also be separate nodes on a LAN.
- 1245 Machine Controller – A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.
- 1250 Modem – A device that allows a computer to communicate through a phone line.
- Management Information System (MIS) – A software system for accessing data from production resources and procedures required to collect, process, and distribute data for use in decision-making.
- 1255 Manufacturing Execution System (MES) – Systems that use network computing to automate production control and process automation. By downloading “recipes” and work schedules and uploading production results, a MES bridges the gap between business and plant-floor or process-control systems.
- 1260 OPC Client/Server – A mechanism for providing interoperability between disparate field devices, automation/control, and business systems.
- 1265 Peer-to-Peer Network – A networking configuration where there is no server and computers connect with each other to share data. Each computer acts as both a client (information or service requestor) and a server (information or service provider).
- 1270 Photo Eye – A light sensitive sensor utilizing photoelectric control that converts a light signal into an electrical signal ultimately producing a binary signal based on an interruption of a light beam.
- Pressure Regulator – A device used to control the pressure of a gas or liquid.
- Pressure Sensor – A sensor system that produces an electrical signal related to the pressure acting on it by its surrounding medium.
- 1275 Primary Domain Controller – A Windows NT server responsible for managing domain information, such as login IDs and passwords.

- 1280 Printer – A device that converts digital data to human readable text on a paper medium.
- Process Controller – A proprietary, typically rack mounted, computer system that processes sensor input, executes control algorithms and computes actuator outputs.
- 1285 Programmable Logic Controller (PLC) – A small industrial computer used in factories originally designed to replace relay logic of a process control system and has evolved into a controller having the functionality of a process controller.
- Proximity Sensor – A non-contact sensor with the ability to detect the presence of a target, within a specified range.
- 1290 Redundant Control Server – A backup to the control server that maintains the current state of the control server at all times.
- 1295 Remote Terminal Unit (RTU) – A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs.
- 1300 Servo Valve – An actuated valve that's position is controlled using a servo actuator.
- Sensor - A device that senses or detects the value of a process variable and generates a signal related to the value. Additional transmitting hardware is required to convert the basic sensor signal to a standard transmission signal. Sensor is defined as the complete sensing and transmitting device.
- 1305 Single Loop Controller – A controller that controls a very small process or a critical process.
- 1310 Solenoid Valve – a valve actuated by an electric coil. A solenoid valve typically has two states: open and closed.
- Supervisory Control and Data Acquisition System (SCADA) – Similar to a Distributed Control System with the exception that sub-control systems are geographically dispersed over large areas.
- 1315 Temperature Sensor – A sensor system that produces an electrical signal related to its temperature and, as a consequence, senses the temperature of its surrounding medium.
- 1320 Variable Frequency Drive (VFD) – A type of drive that controls the speed, but not the precise position, of a non servo, AC motor by varying the frequency of the electricity going to that motor. VFDs are typically used for applications where speed and power are important, but precise positioning is not.
- Workstation – A computer used for tasks such as programming, engineering, and design.

1325

Wide Area Network – A network that spans a larger area than a LAN. A WAN typically provides communications between LANs and may connect to one or more other WANS.

1330

Wireless Device – A device that can connect to a manufacturing system via radio or infrared waves to typically collect/monitor data, but also in cases to modify control set points.